UNITED STATES DISTRICT COURT

for the

Western District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

307 NORTH KENT STREET
WINCHESTER, VIRGINIA 22601

Case No. 5:21mj00022

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Western District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 641	Theft of Public Money
18 U.S.C. 1343	Wire Fraud
18 U.S.C. 1956	Money Laundering

The application is based on these facts:

Please see attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/Peter Dillon
Applicant's signature

Peter Dillon, Special Agent, U.S. Secret Service
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 5/18/21

Judge's signature

City and state: Charlottesville, Virginia

The Honorable Joel C. Hoppe, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
HARRISONBURG DIVISION

IN THE MATTER OF THE SEARCH OF

307 NORTH KENT STREET
WINCHESTER, VIRGINIA 22601

Case No. 5:21mj00022

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Peter Dillon, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises, outbuildings, and curtilage of the location known as 307 North Kent Street, Winchester, Virginia 22601 ("TARGET ADDRESS") located in the City of Winchester, Virginia, within the Western District of Virginia further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the United States Secret Service ("USSS"), and have been since 2017. I am currently assigned to the Washington Field Office, Cyber Fraud Task Force. My duties and responsibilities include the investigation of white collar and financial crimes such as, identity theft and identity crimes, bank fraud, access device fraud, wire fraud, computer fraud, and forgery. I received training in all of the aforementioned disciplines. I am a graduate of the Special Agent Training Course at the USSS James J. Rowley Training Center and the Criminal Investigator Training Program at the Federal Law Enforcement Training Center. Moreover, I am a federal law enforcement officer who is engaged in enforcing the

criminal laws, including 18 U.S.C. §§ 371, 1343, 1349, 1956, and 1956(h), and I am authorized by law to request a search warrant. In the past, I have executed searches of electronic platforms, served a pen register/trap and trace order on internet communications, served 2703(d) court orders, and issued subpoenas for records. I have conducted interviews as part of my criminal investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that Harry Bryce WILLIAMS ("WILLIAMS"), and others, are engaged in a conspiracy, in violation of 18 U.S.C. § 371, theft of public money, in violation of 18 U.S.C. § 641, wire fraud, in violation of 18 U.S.C. § 1343, wire fraud conspiracy, in violation of 18 U.S.C. § 1349, money laundering, in violation of 18 U.S.C. § 1956, and money laundering conspiracy, in violation of 18 U.S.C. § 1956(h). There is probable cause to search the locations described in Attachment A for evidence, contraband, and/or fruits of these crimes further described in Attachment B.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

5. The TARGET ADDRESS is a residence located at 307 North Kent Street, Winchester, Virginia 22601. The residence is described as a white two-story building. The numbers "307" are displayed on a porch post. The TARGET ADDRESS is believed to be the residence of Harry Bryce WILLIAMS and where he resides most often.

PROBABLE CAUSE

Background Information

6. In September 2020, I began investigating an unemployment fraud scheme involving fraud against federal and state unemployment programs. Preliminary information indicated approximate losses totaling $225,338 over a period of months, beginning on or around May 2020. As part of my investigation, Harry Bryce WILLIAMS was discovered to be involved in the scheme. WILLIAMS was the recipient of federal and multiple state unemployment benefits that were obtained in the names of other individuals.

Unemployment Benefits and Financial Accounts of WILLIAMS

City National Bank of West Virginia

7. In September 2020, law enforcement subpoenaed City National Bank of West Virginia for accounts belonging to WILLIAMS. Documents produced included an account ending in -6778 for Harry B. WILLIAMS of 307 North Kent Street, Winchester, Virginia.

8. The statements for account -6778 had 30 deposits totaling $23,490 on May 18, 2020, and eight deposits totaling $6,336 on May 21, 2020, with the description "Deposit CARES Act MA DUA." MA DUA is the Massachusetts Department of Unemployment Assistance and the CARES Act is a Massachusetts benefit program that includes unemployment assistance and compensation.

9. The same day as the deposits totaling $23,490, WILLIAMS signed a withdrawal slip totaling $3,900.00 for account -6778. On May 19, 2020, $20,000 was wired to beneficiary New Watson Doors Industry Inc at an account ending in -0758. On or between May 20 and May 26, account -6778 was debited $3,870 at TransferWise, $100 at Sheetz, and $35 in peer-to-peer (P2P) transactions.

10. On June 12, 2020, the statement for account -6778 listed a deposit for $5,960 with the description "UI Benefit UIA Pre-Paid." This description is associated with the Michigan Unemployment Insurance Agency. This deposit was reversed on July 30, 2020. Additionally, $11,798.17 was also reversed on July 30, 2020. This reversal had the description "State of Mass UE Fraud."

PNC and COVID-19 Economic Injury Disaster Loan (EIDL)

11. Under the provisions of The CARES Act, $2.2 trillion dollars in economic stimulus was passed by the 116th U.S. Congress and signed into law by President Donald Trump in March 2020 in response to the economic decline caused by the COVID-19 pandemic in the United States.

12. The provisions of The CARES Act, in conjunction with an officially declared disaster by the United States Government, allowed for the U.S. Small Business Administration (SBA) to offer EIDL funding to business owners negatively affected by the COVID-19 pandemic. Using the SBA online portal, EIDL applicants submit personal and business information in support of each EIDL application, and they do not have to submit supporting documentation of any sort.

13. The application includes a jurat-like paragraph where the applicant affirms that the information submitted is true and correct under the penalty of perjury and applicable criminal statutes. The application process involves filling out assorted data fields relating to the size of the affected business entity, the ownership of said business, and other information such as the number of employees and gross business revenues realized in the 12 months prior to COVID-19 impact on the national economy. This information, submitted by the applicant, is then used by SBA systems to calculate the principle amount of money the small business is

eligible to receive in the form of an EIDL. However, in conjunction with the submission of an EIDL application, by simply clicking on and checking a box within the on-line application, an applicant may request and then receive up to $10,000.00 in an EIDL Cash Advance Grant based on the number of employees claimed. The EIDL Cash Advance Grant need not be repaid to the SBA if the loan application is ultimately denied by the SBA, or if the applicant declines the EIDL that may be offered by the SBA at a later date.

14. The SBA Office of Disaster Assistance (ODA) controls the EIDL program and is headquartered at 409 3rd Street SW, Washington, DC 20416. The ODA has authority over all loans created and disbursed under the EIDL program. EIDL proceeds and available Cash Advance Grants (up to $10,000) are solely funded by the SBA and are disbursed from government-controlled accounts maintained with the U.S. Treasury at Federal Reserve Banks throughout the United States.

15. Pursuant to the provisions governing the EIDL program, loan proceeds must be used by that business on certain permissible expenses. The EIDL (working capital) loans may be used by the afflicted business, which must have existed in an operational condition on February 1, 2020, to pay fixed debts, payroll, accounts payable, and other bills that could have been paid had the COVID-19 disaster not occurred.

16. In September 2020, law enforcement subpoenaed PNC Bank for accounts belonging to WILLIAMS. Documents produced included an account ending in -5129, a PNC SmartAccess Prepaid Visa Card for Harry B. WILLIAMS of 307 North Kent Street, Winchester, Virginia.

17. The statement for this account shows that on June 23, 2020, there was a credit of $140,700 with the description “SBAD TREAS 310 Misc Pay.” The description SBAD Treas

means the payment is from the United States Treasury and affiliated with the SBA. ACH details for this transaction list the associated individual as T.P. and the "Orig Stat" field lists "Fed Govt."

18. In September 2020, the SBA Office of Inspector General provided documents regarding the above payment. The payment was part of an SBA COVID-19 disaster loan for economic injury for a borrower identified as T.P. (born 1956).

SoFi

19. In September 2020, law enforcement subpoenaed SoFi for accounts belonging to WILLIAMS. Documents produced included an account ending in -1230 for Harry B. WILLIAMS of 307 North Kent Street, Winchester, Virginia. The statements for account -1230 show the following:

20. May 12, 2020, one deposit for $8,928.00 with the description "WA ST Employ SEC UI Benefit." WA ST Employ SEC UI Benefit is the Washington State Employment Security Department. Following the $8,928 deposit, on or between May 12 and May 16, the account was debited $4,030 at Walmart, $92.63 at AutoZone, and $3,800 was withdrawn at ATMs.

21. May 21, 2020, four deposits totaling $15,667.00 with the description "Maine Dept Labor UNEMP COMP." Maine Dept Labor UNEMP COMP is the Maine Department of Labor's Bureau of Unemployment Compensation. Following the four deposits totaling $15,667, on or between May 21 and May 25, the account was debited $2,855.25 at the U.S. Postal Service, $3,150 at Walmart, $5,616.68 at Martin's Food, $15 at CITGO, and $4,000 was withdrawn at ATMs.

a. In November 2020, copies of three money orders totaling $2,850 (26654053138 for $1,000, 26654053140 for $1,000, and 26654053151 for $850) were obtained from the U.S. Postal Inspection Service (USPIS). These correspond to the above debit of $2,855.25. The higher debit total on the statement is due to the fees charged for the money orders.

b. In November 2020, receipts were obtained from Martin's Food parent company, Ahold USA, showing that the previously mentioned Martin's Food transactions included the below purchases or cash back transactions:

- 08:03 on May 21, 2020, at store 6078, $200 cash back
- 17:28 on May 22, 2020, at store 6078, $200 cash back
- 17:38 on May 22, 2020, at store 6077, $200 cash back
- 18:33 on May 24, 2020, at store 6078, $3,000 in money orders
- 08:24 on May 25, 2020, at store 6283, $1,500 in money orders, $200 cash back

22. June 5, 2020, ten deposits totaling $9,100.00 with the description "Wisconsin-DWD-UI UI-Payment." Wisconsin-DWD-UI UI-Payment is the Wisconsin Department of Workforce Development. Following the deposits totaling $9,100, on or between June 5 and June 7, the account was debited $4,007 at the U.S. Postal Service, $12.55 at Sunoco, $14.17 at Walmart, $24.49 at Martin's Food, $1,012 at Credit Acceptance Corp, and $4,000 was withdrawn at ATMs.

a. In November 2020, copies of four money orders totaling $4,000 (26654059192 for $1,000, 26654059203 for $1,000, 26654059214 for $1,000, and 26654059225 for $1,000) were obtained from the USPIS.

These correspond to the above debit of $4,007. The higher debit total on the statement is due to the fees charged for the money orders.

23. June 9, 2020, one deposit for $7,170.00 with the description "State of Arizona Benefitpay." State of Arizona Benefitpay is the Arizona Department of Administration's Benefit Services Division. Following the $7,170 deposit, on or between June 9 and June 15, the account was debited $1,022.92 at Martin's Food, $18.30 at Bojangles', $4.69 at Bo's Express, $9.72 at 7-Eleven, $12.22 at KFC, $7.79 at McDonald's, $2,022.96 at Credit Acceptance Corp, and $4,050 was withdrawn at ATMS.

a. In November 2020, receipts were obtained from Martin's Food parent company, Ahold USA, showing that the previously mentioned Martin's Food transactions included the below purchases or cash back transactions:

- 20:06 on June 09, 2020, at store 6078, $100 Amazon gift card (6169594514850356), and $200 cash back
- 20:07 on June 09, 2020, at store 6078, $100 Amazon gift card (6177900499870881), and $200 cash back
- 15:49 on June 10, 2020, at store 6078, $200 cash back
- 15:51 on June 10, 2020, at store 6078, $200 cash back

TD Bank

24. In December 2020, law enforcement subpoenaed TD Bank for accounts belonging to WILLIAMS. Documents produced included an account ending in -4602 for Bryce WILLIAMS and an account ending in -0942 for Harry B WILLIAMS. The two account holders share the address 307 North Kent Street, Winchester, Virginia, and listed the same Social

Security Number and date of birth, i.e. Harry B WILLIAMS and Bryce WILLIAMS are the same individual.

25. The statement for account -4602 shows a deposit for $7,770.00 on July 13, 2020, with the description "IDES Payments xxxxx6421." IDES is the Illinois Department of Employment Security. Following the $7,770 deposit, on or between July 13 and July 17, the account was debited $300 at Sheetz, $52.30 at Martin's Food, $37.69 at Golden Corral, $1,050 at TransferWise, $4,000 for Zelle P2P transfers to Woodforest National Bank, $20.43 at McDonald's, $12.10 at Bo's Xpress, and $2,000 was withdrawn at ATMs.

26. The statement for account -4602 shows two deposits totaling $5,370.00 (each for $2,685) on August 18, 2020, with the description "State of Arizona Benefitpay." As previously mentioned, this is the Arizona Department of Administration's Benefit Services Division. Following these two deposits totaling $5,370, on or between August 18 and August 21, the account was debited $5,000 due to a transfer to WILLIAMS' TD account -0942, $30 at Bo's Xpress, $200 at Sheetz, $18.23 at McDonald's, $20.87 at 7-Eleven, $31.53 at Pep Boys, and $33.87 at Roy Rogers.

27. The statement for account -0942 shows the above transfer of $5,000 from -4602 on August 18, 2020, and two previous transfers, $1,000 on August 10, 2020, and $18,000 on August 11, 2020. Following the transfer to -0942 on August 18, 2020, there was no further activity on the account until September 3. On or between September 3 and September 8, the account was debited $21.21 at Roy Rogers, $247.68 at Walmart, $1,950 at Winchester Eye Surgery, $2,395.70 at Santander, $379.02 at Amazon, $77.93 at Golden Corral, $200 at Sheetz, $112.29 at Martin's Food, and $4,000 was withdrawn at ATMs.

Woodforest National Bank

28. In September 2020, law enforcement subpoenaed Woodforest National Bank for accounts belonging to WILLIAMS. Documents produced included an account ending in -9278 and an account ending in -9146, both for Harry B. WILLIAMS of 307 North Kent Street, Winchester, Virginia.

29. The statement for account -9278 shows two deposits from "Benefitpay [S.G.] State of Arizona," one for $7,170.00 on June 09, 2020, and another for $1,230.00 on June 10, 2020. The payments were reversed on June 9 and June 16. No further activity took place between the deposits and the reversals.

State Benefit Agencies

Massachusetts Department of Unemployment Assistance

30. In September 2020, the Massachusetts Department of Unemployment Assistance, Pandemic Unemployment Program provided the USSS with documentation regarding benefit payments to WILLIAMS. The payments to WILLIAMS' City National Bank account -6778 are linked to four identities. For the deposits on May 18, 2020, totaling $23,490: $7,020 is linked to identity C.T. (born 1945), $7,020 is linked to J.C. (born 1953), and $9,450 is linked to J.C. (born 1957). The deposits on May 21, 2020, totaling $6,336, are linked to identity G.B. (born 1991).

Washington State Employment Security Department

31. In September 2020, the Washington State Employment Security Department provided the USSS with documentation regarding benefit payments to WILLIAMS. The payments to WILLIAMS' SoFi account -1230 are all linked to an application under the identity

of J.F. (born in 1968). The application was for a total of $9,920, but due to taxes, only $8,928 was deposited in WILLIAMS' account.

Wisconsin Unemployment Insurance

32. In September 2020, the Wisconsin Department of Workforce Development, Unemployment Insurance provided the USSS with documentation regarding benefit payments to WILLIAMS. The payments to WILLIAMS' SoFi account -1230 are all linked to an application from one identity, T.S. Record checks show that T.S. was born in 1961. There were four additional identities with applications linked to account -1230, but no payments were made from these applications.

Arizona Department of Economic Security

33. In December 2020, the Arizona Department of Economic Security (DES), Office of Inspector General (OIG) provided the USSS with documentation regarding benefit payments to WILLIAMS. Seven identities had applications linked to WILLIAMS SoFi account -1230. Of the seven identities linked to the SoFi account, only one resulted in a payment (identity S.B., born 1957). One identity had an application linked to WILLIAMS' Woodforest National Bank account -9278, identity S.G. (born 1956). As previously mentioned this resulted in two deposits to the Woodforest account that were later reversed.

Summary Table

34. The below table summarizes the deposits to WILLIAMS' accounts

Post Date	Amount	Destination Account of WILLIAMS	Source of Funds	Applicant Identity Age 60 or Older
05/18/20	$23,490	City National Bank of WV -6778	Massachusetts	Yes
05/21/20	$6,336	City National Bank of WV -6778	Massachusetts	No

06/12/20	$5,960	City National Bank of WV -6778	Michigan	Unknown
06/23/20	$140,700	PNC -5129	U.S. SBA	Yes
05/12/20	$8,928	SoFi -1230	Washington	No
05/21/20	$15,667	SoFi -1230	Maine	Unknown
06/05/20	$9,100	SoFi -1230	Wisconsin	Yes
06/09/20	$7,170	SoFi -1230	Arizona	Yes
07/13/20	$7,770	TD -4602	Illinois	Unknown
08/18/20	$5,370	TD -4602	Arizona	Unknown
06/09/20	$7,170	Woodforest National Bank -9278	Arizona	Yes
06/10/20	$1,230	Woodforest National Bank -9278	Arizona	Yes
$238,891 in total deposits to accounts controlled by WILLIAMS (May 2020 to August 2020)				

Income and Vehicle Purchase

35. In February 2021, law enforcement subpoenaed Santander Consumer USA Inc. (Santander) for accounts belonging to WILLIAMS. Documents produced included an automobile loan account ending in -5217 for Harry B. WILLIAMS of 307 North Kent Street, Winchester, Virginia, for a 2020 Nissan Rogue purchased on July 16, 2020. According to the documents, WILLIAMS made a cash deposit of $3,500 for the vehicle and the final balance due was $23,643.20. The 72-month payment schedule for the vehicle lists the monthly payment amount as $598.04. The previously discussed debits from WILLIAMS' TD account appear in the Santander payment records.

36. WILLIAMS supplied Santander with paystubs for his work at Kingsdown, Inc. (gross pay of $1,531.09 and net pay of $760.84 in the two week pay period ending July 11, 2020) and Texas Roadhouse (gross pay of $854.04 and net pay of $707.98 in the one week pay period ending July 07, 2020). In documents filed with the Virginia Employment Commission in

May 2020, WILLIAMS listed his annual gross salary with Kingsdown, Inc. as $30,000 and $21,000 for Texas Roadhouse, for a total sum of $51,000.

Withdrawals/Debits from WILLIAMS' Accounts

37. The previously described ATM withdrawals that followed the deposits of unemployment benefits (from Massachusetts, Washington, Maine, Wisconsin, Arizona, and Illinois), conducted in May, June, and September 2020, total $27,350 in cash.

38. Payments to Credit Acceptance Corp, conducted in June 2020 from WILLIAMS' SoFi account -1230, following the deposit of Wisconsin and Arizona unemployment benefits, total $3,034.96. A search for Credit Acceptance Corp shows that it is a vehicle finance company. Records from Santander show that when WILLIAMS purchased his Nissan Rogue, he traded-in a Nissan Altima. Santander records noted it as "Credit Acceptance Trade" and a payoff to "Credit Acceptance."

39. As previously stated, in September 2020, after the deposit of Arizona unemployment benefits to WILLIAMS' TD -4602 and a transfer of funds to WILLIAMS' TD -0942, WILLIAMS paid $2,395.70 to Santander, his lender for the purchase of a 2020 Nissan Rogue. Records from Santander show that $1,195.10 of the $2,395.70 was returned to WILLIAMS' TD account (due to overpayment). During this same time and from the same account, WILLIAMS paid $1,950 to Winchester Eye Surgery.

40. The cash withdrawals, car payments (not including the returned $1,195.10), and eye surgery payments, conducted on or between May 2020 and September 2020, total $33,535.56.

Fraud Scheme and Money Laundering Communications

41. Based on my training and experience, fraud schemes and money laundering often involve multiple actors or teams of actors. For instance, one individual completes a fraudulent claim, another individual sets up bank accounts for the receipt of funds and moves the funds into another form (e.g. money orders, cash, gift cards), and another individual cashes these proceeds and further distributes proceeds. In addition to traditional methods of communication, such as using the phone, fraud actors have been known to use newer forms of communication, such as text messages and applications (e.g. Instagram, WhatsApp, and Telegram).

The TARGET ADDRESS

42. The TARGET ADDRESS is believed to be the residence of WILLIAMS. WILLIAMS' Virginia driver's license, T63135434, lists his address as 307 North Kent Street, Winchester, Virginia. WILLIAMS' vehicle, a 2020 Nissan, is registered in his name at the 307 North Kent Street, Winchester, Virginia, address.

43. The bank accounts used by WILLIAMS as part of the fraud scheme list the TARGET ADDRESS as his residence. These financial institutions maintain the TARGET ADDRESS for mailing purposes and likely send statements and other documents concerning their financial activity to the TARGET ADDRESS.

44. On May 10, 2021, law enforcement observed WILLIAMS' vehicle across the street from the TARGET ADDRESS. On May 11, 2021, law enforcement observed WILLIAMS' vehicle in front of the TARGET ADDRESS.

SUMMARY

45. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that Harry Bryce WILLIAMS, and others, have violated Title 18,

United States Code, Sections 641, 1343, 1349, 1956, and 1956(h), to wit: theft of public money, wire fraud, wire fraud conspiracy, money laundering, and money laundering conspiracy, and that electronic devices, communication devices, computers, documentation, and other items related to the fraud scheme will be located in the residence at the TARGET ADDRESS.

46. Based on the aforementioned, your affiant respectfully submits that there is probable cause to believe that U.S. Currency, documentation, and/or other items related to the fraud scheme and money laundering further described in Attachment B will be located at the TARGET ADDRESS.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

47. As described above and in Attachment B, this application seeks permission to search for records that might be found at the TARGET ADDRESS, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

48. *Probable cause.* I submit that if a computer or storage medium is found at the TARGET ADDRESS, there is probable cause to believe relevant records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted,

they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the Crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any storage medium in the TARGET ADDRESS because:

d. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

e. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the Criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet

history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the Crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence

of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a Crime (e.g., internet searches indicating Criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

f. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

g. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

i. I know that when an individual uses a computer to communicate online with a victim in a fraud scheme, the individual's computer will generally serve both as an instrumentality for committing the Crime, and also as a storage medium for evidence of the Crime. The computer is an instrumentality of the Crime because it is used as a means of committing the Criminal offense. The computer is also likely to be a storage medium for evidence of Crime. From my training and experience, I believe that a computer used to commit a Crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the Criminal conduct was achieved; records of Internet discussions about the Crime; and other records that indicate the nature of the offense.

50. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make

an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the

storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

51. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

52. Based on my training, experience, and the foregoing facts set forth herein, I believe that probable cause exists to search the address described in Attachment A to seize items described in Attachment B.

53. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A, in order to seek the items described in Attachment B.

OATH

I declare under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,

s/Peter Dillon
Peter Dillon, Special Agent
United States Secret Service

Received by reliable electronic means and sworn and attested to by telephone on this 18th day of May 2021.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE

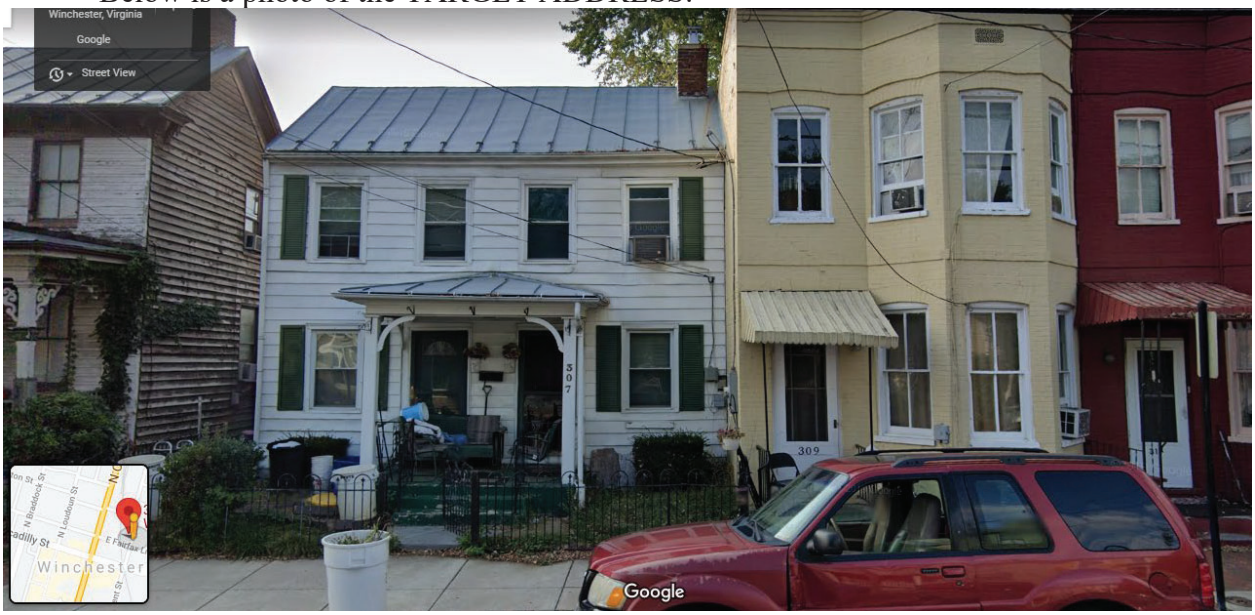
ATTACHMENT A

Place and Property to Be Searched

The property to be searched is a residence located at 307 North Kent Street, Winchester, Virginia 22601 (TARGET ADDRESS) in the City of Winchester. The residence is described as a white two-story building. The numbers "307" are displayed on a porch post.

This application is for a warrant to search the residences described herein and all outbuildings and vehicles on or within the curtilage of each property.

Below is a photo of the TARGET ADDRESS:



ATTACHMENT B

Property to be Seized

1. All records relating to violations of conspiracy in violation of 18 U.S.C. § 371, theft of public money, in violation of 18 U.S.C. § 641, wire fraud, in violation of 18 U.S.C. § 1343, wire fraud conspiracy, in violation of 18 U.S.C. § 1349, money laundering, in violation of 18 U.S.C. § 1956, and money laundering conspiracy, in violation of 18 U.S.C. § 1956(h), those violations involving Harry Bryce WILLIAMS ("WILLIAMS"), and his coconspirators, including:

   a. Any documents related the financial activity of WILLIAMS, or other co-conspirators, including, but not limited to, bank statements, general journals and ledgers, accounts payable, accounts receivable, payroll ledgers, invoices, receipts, bank statements, deposit slips, canceled checks, check stubs, withdrawal slips, credit card statements, loan and line of credit documents, income tax returns and related documents, and or related correspondence;

   b. Photographs, including still photographs, negatives, video tapes, films, undeveloped film and the contents therein, slides, in particular photographs of co-conspirators and/or assets;

   c. Address and/or telephone books, rolodex indices and any papers reflecting names, addresses, telephone numbers, pager numbers, fax machines, and/or telex numbers of co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;

   d. Indicia of occupancy, residency, rental, and/or ownership of the premises to be searched, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase, or lease agreements, and keys;

   e. Any conversations, whether through text messages or other applications, concerning public money, benefit payments, fraud schemes, and money laundering;

   f. All bank records, checks, credit card bills, account information, and other financial records;

   g. Records and information relating to the identity or location of the suspects;

h. United States currency, precious metals, jewelry, and financial instruments, including stocks and bonds;

i. Books, records, invoices, receipts, records of real estate transactions (whether rented or owned property), bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, and cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transferring, and/or concealment of assets and the obtaining, secreting, transferring, concealing, and/or expending of money;

j. Electronic equipment, such as cellular telephones (and the data contained within), computers, telex machines, facsimile machines, currency counting machines, and telephone answering machines (including listening to any messages recorded on such machines). Additionally, computer software, tapes, discs, CD, DVDs, audio tapes, and the contents therein, containing the information generated by the aforementioned electronic equipment.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.